Abstract

Information is central to healthcare: for proper care, information must be shared. Modern healthcare is highly collaborative, involving interactions between users from a range of institutions, including primary and secondary care providers, researchers, government and private organisations. Each has specific data requirements relating to the service they provide, and must be informed of relevant information as it occurs.

Personal health information is highly sensitive. Those who collect/hold data as part of the care process are *responsible* for protecting its confidentiality, in line with patient consent, codes of practice and legislation. Ideally, one should receive only that information necessary for the tasks they perform—on a *need-to-know* basis.

Healthcare requires mechanisms to strictly control information dissemination. Many solutions fail to account for the scale and heterogeneity of the environment. Centrally managed data services impede the local autonomy of health institutions, impacting security by diminishing accountability and increasing the risks/impacts of incorrect disclosures. Direct, synchronous (request-response) communication requires an enumeration of every potential information source/sink. This is impractical when considering health services at a national level. Healthcare presents a data-driven environment highly amenable to an event-based infrastructure, which can inform, update and alert relevant parties of incidents as they occur. Event-based data dissemination paradigms, while efficient and scalable, generally lack the rigorous access control mechanisms required for health infrastructure.

This dissertation describes how *publish/subscribe*, an asynchronous, push-based, many-to-many middleware communication paradigm, is extended to include mechanisms for actively controlling information disclosure. We present *interaction control*: a data-control layer above a publish/subscribe service allowing the definition of context-aware policy rules to authorise information channels, transform information and restrict data propagation according to the circumstances. As dissemination policy is defined at the broker-level and enforced by the middleware, client compliance is ensured. We build interaction control mechanisms into integrated database-brokers to provide a rich representation of state; while facilitating audit, which is essential for accountability.

Healthcare requires the sharing of sensitive information across federated domains of administrative control. Interaction control provides the means to balance the competing concerns of information sharing and protection. It enables those responsible for information to meet their data management obligations, through specification of fine-grained disclosure policy.